The bounded round quantum communication complexity of set disjointness

Speaker: Jaikumar Radhakrishnan, Tata Institute, Mumbai

Joint work with

Rahul Jain, Cadence, New Delhi

Pranab Sen, University of Waterloo

Set disjointness

A $\qquad\qquad\qquad\qquad$ B

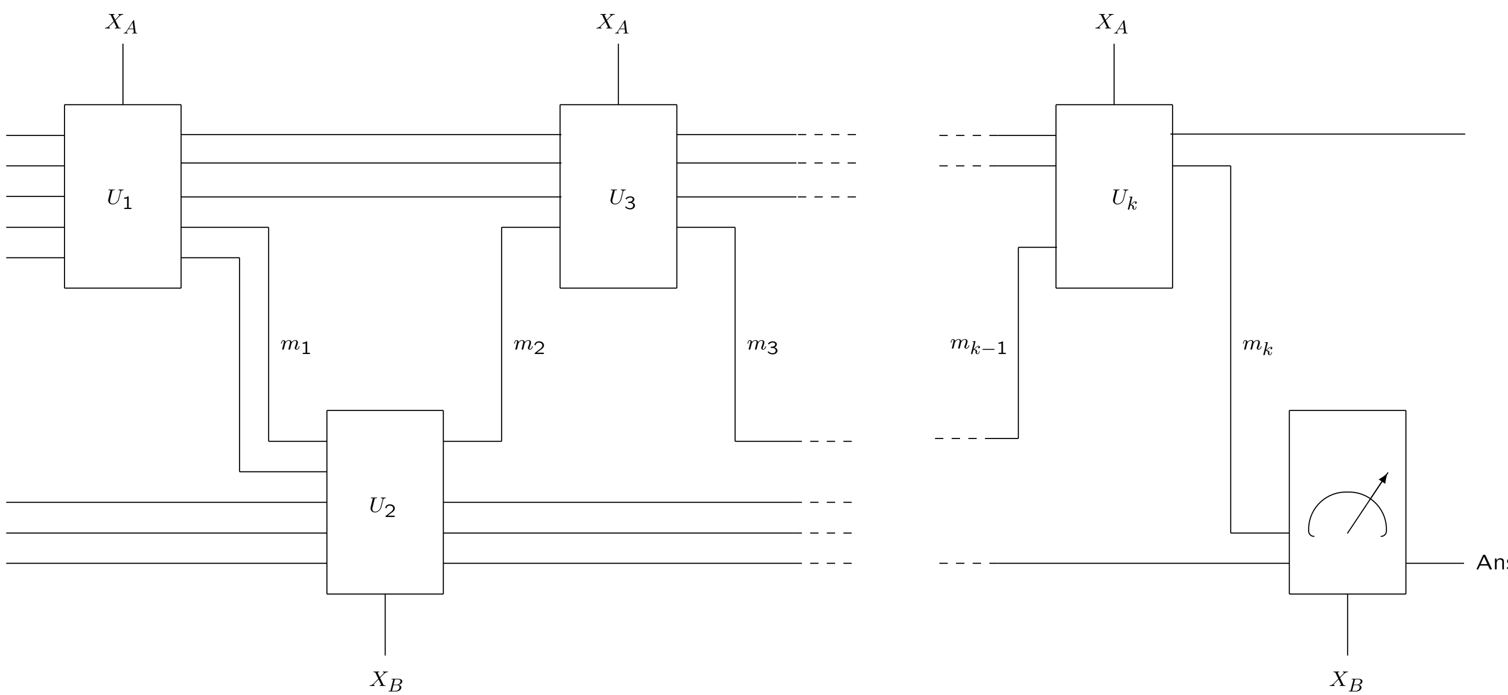
$X_A \subseteq [n]$ $\qquad\qquad\qquad\qquad$ $X_B \subseteq [n]$

B needs to determine if $X_A \cap X_B \stackrel{?}{=} \emptyset$.

$$f(X_A, X_B) \stackrel{\text{def}}{=} \bigvee_{i=1}^{n} (X_A[i] \wedge X_B[i]).$$

Optimal deterministic protocol: A sends n bits to B.

Quantum protocols (Yao 1993)



Answer should be correct with probability $\geq 2/3$.

Goal: Minimise $m_1 + m_2 + \ldots + m_k$.

Classical randomised protocols

(error $\leq 1/3$)

Babai, Frankl and Simon 1986:	$\Omega(\sqrt{n})$
Kalyanasundaram and Schnitger 1992:	$\Omega(n)$
Razborov 1992:	$\Omega(n)$
Bar-Yossef, Jayram, Kumar and Sivakumar 2002:	$\Omega(n)$

Question: Do quantum protocols fare better?

Quantum protocols

(error $\leq 1/3$)

Buhrman, Cleve and Wigderson 1998:	$O(\sqrt{n}\log n)$
Hoyer and de Wolf 2002:	$\sqrt{n}2^{O(\log^* n)}$
Klauck, Nayak, Ta-Shma and Zuckerman 2001:	$\Omega(n^{1/k})$
Razborov 2003:	$\Omega(\sqrt{n})$
Aaronson and Ambainis 2003:	$O(\sqrt{n})$

In this talk

Q. Is there a 3-round optimal quantum protocol?

Q. How well can one do with k-round quantum protocols?

k-round quantum protocols

Aaronson and Ambainis 2003

$$\Downarrow$$

$O\left(\frac{n}{k}\log\frac{n}{k^2}\right)$-qubit k-round protocol.

Today

In any k-round quantum protocol for set disjointness, A and B must exchange $\Omega(n/k^2)$ qubits.

Plan of the talk

Review of Bar-Yossef et al. (2002)

Part 1: Reduction to AND (information-theoretic)

Part 2: Lower bound for AND

The quantum proof.

Part 1: Reduction to AND (almost the same as before)

Part 2: Lower bound for AND using round elimination.

From disjointness . . . to AND

$\boxed{\text{An } m\text{-qubit } k\text{-round protocol for disjointness.}}$

$$\Downarrow$$

An m-qubit k-round protocol for AND of two bits where neither party reveals more than $\frac{m}{n}$ bits of information about his input *when* the other party has input 0.

Distributions on inputs

For $j = 1, 2, \ldots, n$, one party gets 0 and the other party a random bit:

$$X_A[j] = 0 \text{ and } X_B[j] \text{ is random}$$

or

$$X_B[j] = 0 \text{ and } X_A[j] \text{ is random}$$

There are 2^n such distributions. The sets X_A and X_B are always disjoint, so the answer is 0.

Information theory . . .

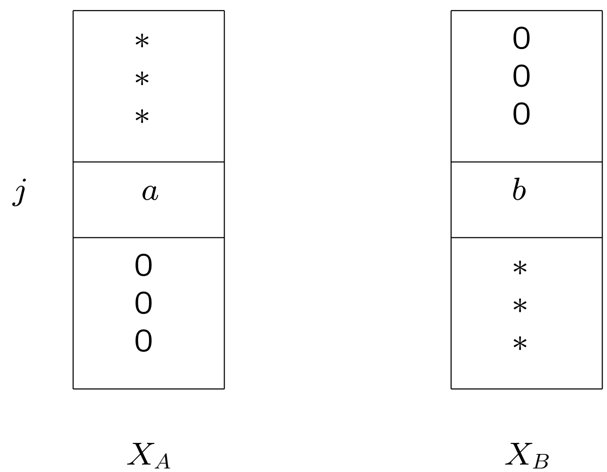
For each such distribution consider the mutual information between the input and the transcript ($\stackrel{\text{def}}{=}$ concatenation of all the messages).

$$\begin{aligned} I[X_A : \mathsf{transcript}] &\leq |\mathsf{transcript}| \leq m \\ I[X_B : \mathsf{transcript}] &\leq |\mathsf{transcript}| \leq m. \end{aligned}$$

$X_A[j]$ are independent:

$$\sum_{j=1}^{n} I[X_A[j] : \mathsf{transcript}] \leq I[X_A : \mathsf{transcript}] \leq m.$$

The protocol has a weak coordinate j



If $X_B[j] = 0$ and $X_A[j]$ is random $I[X_A[j] : \text{transcript}] \leq \frac{m}{n}$.
If $X_A[j] = 0$ and $X_B[j]$ is random $I[X_B[j] : \text{transcript}] \leq \frac{m}{n}$.

The protocol is neglecting the jth coordinate!

Lemma 1

There is an m-bit protocol for disjointness

$$\Downarrow$$

There is an m-bit protocol for computing the AND of two bits a and b where

- if $a = 0$ and b is random, then

$$I[b : \text{transcript}] \leq \frac{m}{n}.$$

- if $b = 0$ and a is random, then

$$I[a : \text{transcript}] \leq \frac{m}{n}.$$

Lemma 2

There is a constant $c > 0$ such that in any protocol for AND

$$I[a : \text{transcript} \mid b = 0] \geq c \quad \text{or} \quad I[b : \text{transcript} \mid a = 0] \geq c.$$

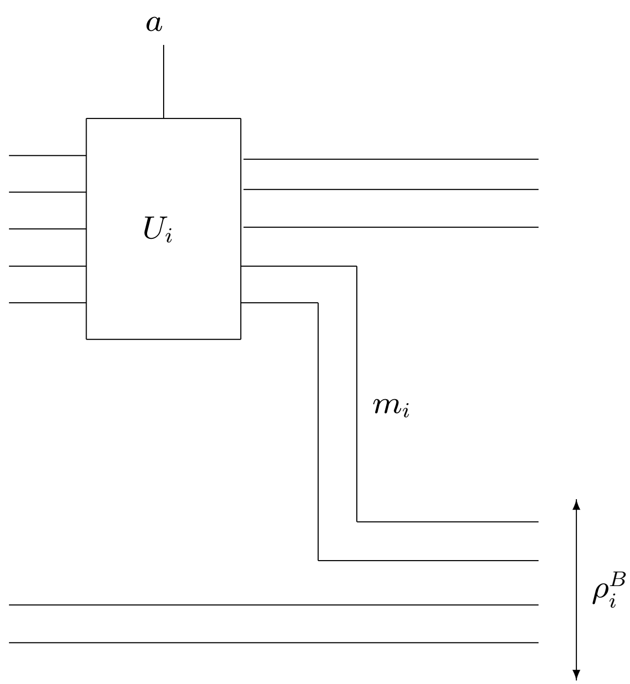
$$\boxed{\text{Lemma 1 + Lemma 2}}$$

$$\Downarrow$$

$$\boxed{\begin{aligned} \frac{m}{n} &\geq c \\ m &= \Omega(n). \end{aligned}}$$

A quantum analogue of the argument?

How does one define information between inputs and the transcript in quantum protocols?



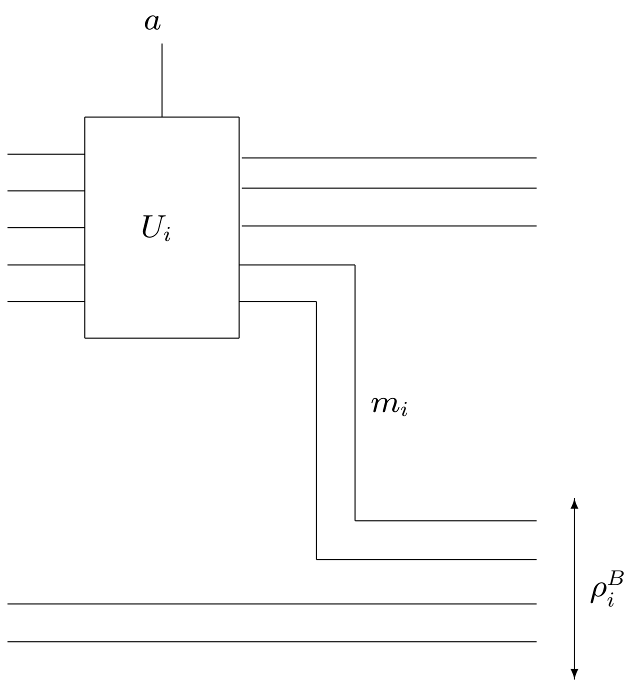
From disjointness to AND . . .

$$2m \geq I[X_A : \rho_i^B] \geq \sum_{j=1}^{n} I[X_A[j] : \rho_i^B].$$

(Using Cleve et al. 1998.)

Lemma 1: There is a quantum protocol for AND where neither party leaks more than $\frac{m}{n}$ bits of information about his input when the other party has input 0.

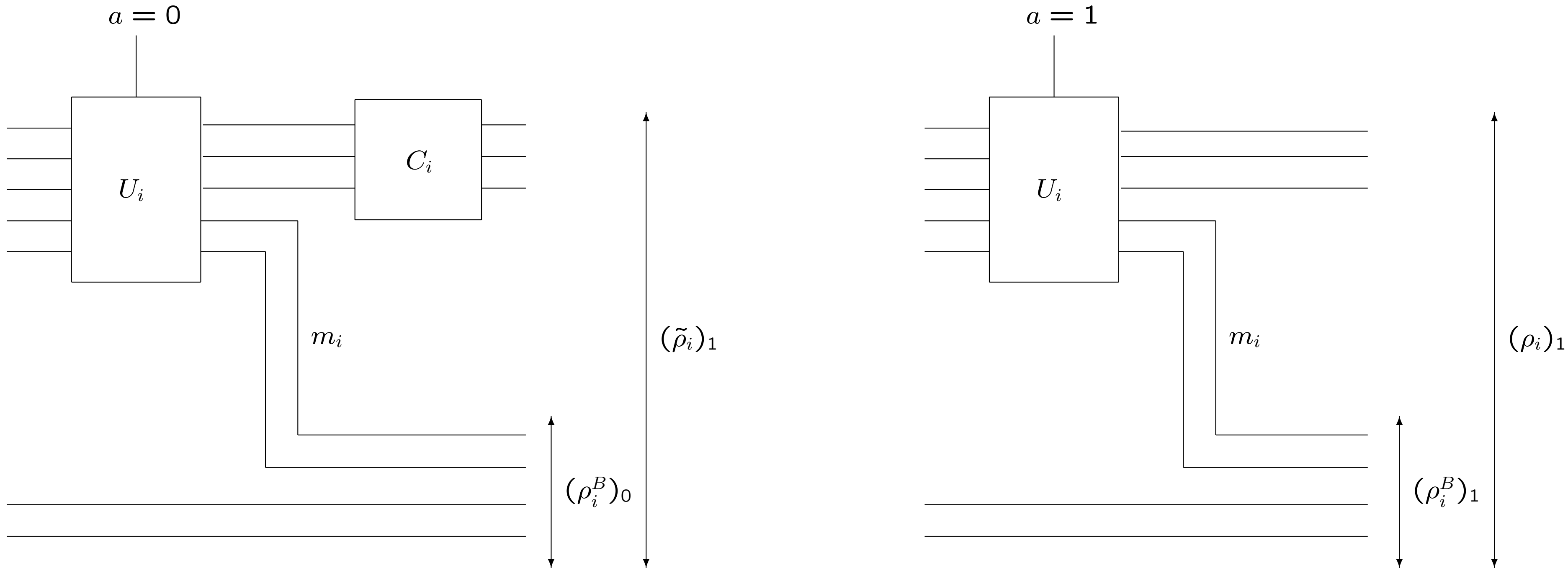
The protocol for AND



$$
\begin{aligned}
I_1 &\stackrel{\text{def}}{=} I[a : \rho_1^B \mid b = 0] \\
I_2 &\stackrel{\text{def}}{=} I[b : \rho_2^A \mid a = 0] \\
&\vdots \\
I_k &\stackrel{\text{def}}{=} I[a : \rho_k^B \mid b = 0].
\end{aligned}
$$

We have ensured that $I_1, I_2, \ldots, I_k \leq \frac{m}{n} \stackrel{\text{def}}{=} \epsilon$.

Local transition

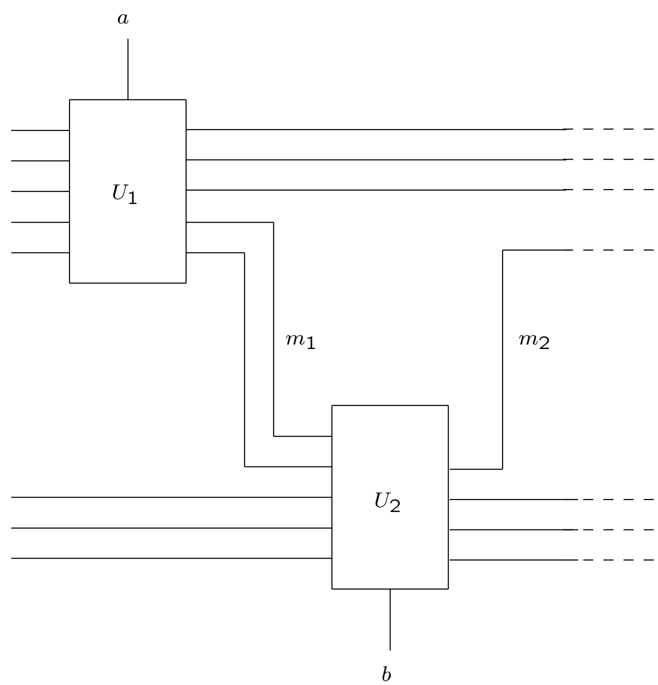


Information about a in ρ_i^B less than ϵ

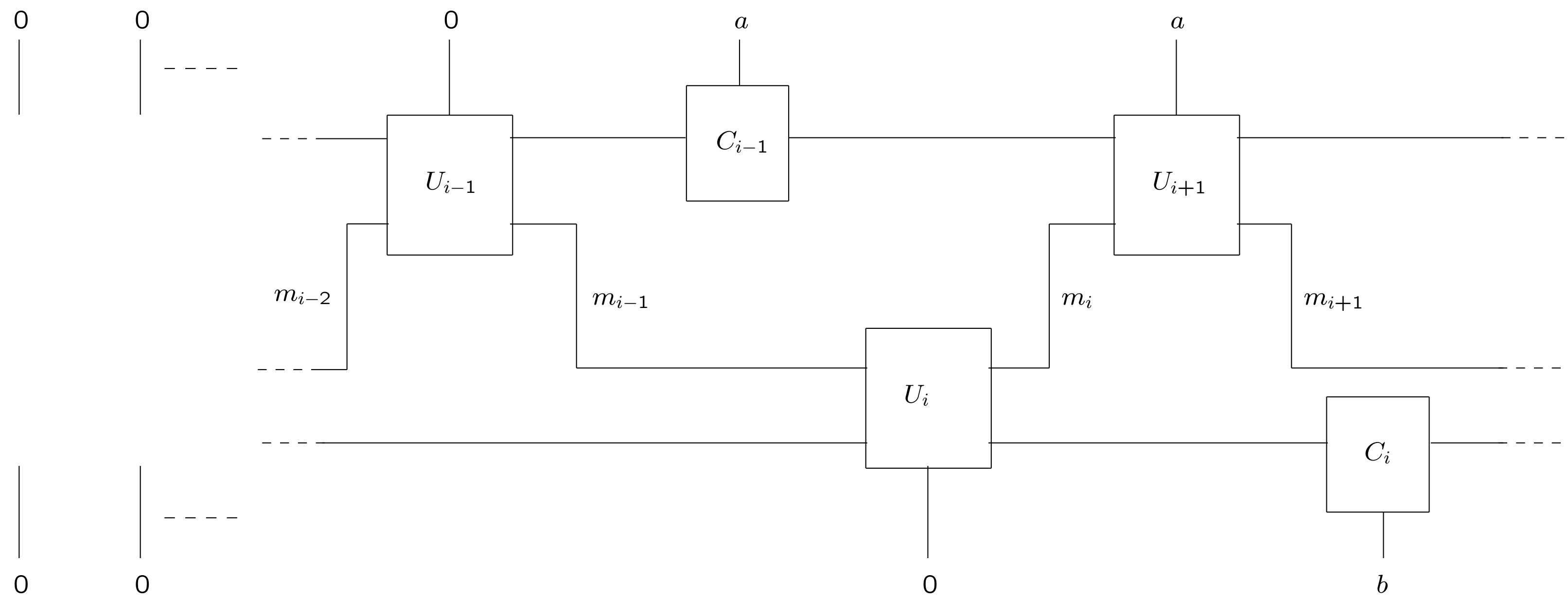
$$\Downarrow$$

$$\exists C_i : \|(\rho_i)_1 - (\tilde{\rho}_i)_1\|_t \leq \sqrt{\epsilon}.$$

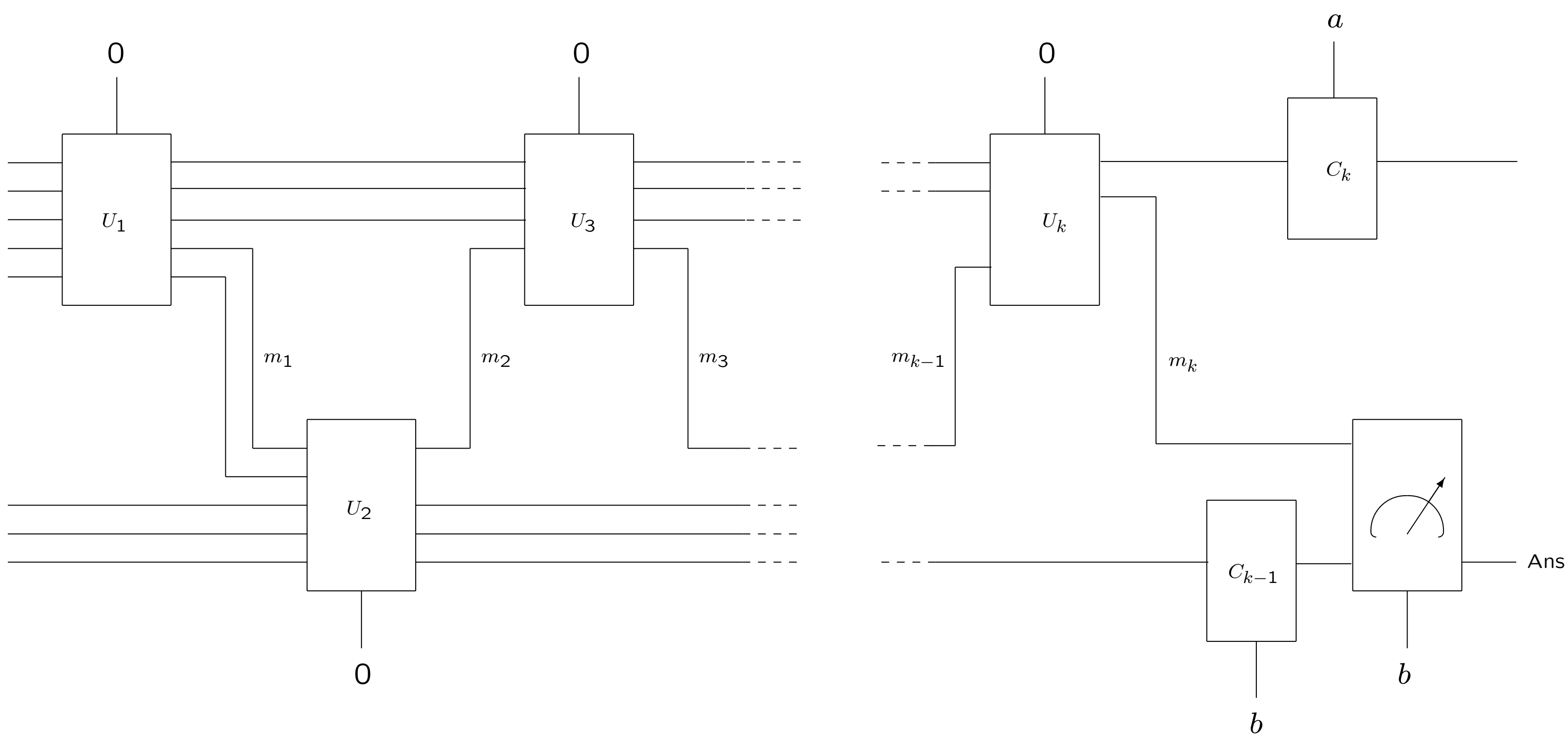
Eliminating rounds 1 and 2



Eliminating round i



The final protocol for AND



Prob. of error $\leq \frac{1}{3} + k\sqrt{\epsilon}$.

A's messages do not depend on a!

Set $b = 1$; so, the AND of a and b is a. But B cannot predict a with probability better than $\frac{1}{2}$.

$$k \cdot \sqrt{\epsilon} \geq \text{const.} \Rightarrow k \cdot \sqrt{\frac{m}{n}} \geq \text{const.}$$

Thus, $m = \Omega(\frac{n}{k^2})$.

Summary

Step 1: From an m-qubit k-round protocol for disjointness, derive a protocol for AND where the party with input 0 gets very little information about the input of the other party.

Tool: $I[X : \rho] \geq \sum_j I[X[j] : \rho]$. (Mimics Bar-Yossef et al.)

Step 2: Any such protocol for AND must leak $\Omega(\frac{1}{k^2})$ bits of information per round.

Tools: Round elimination, fidelity, local transition. (Inspired by Klauck et al.)

Finally . . .

In any k-round quantum protocol for set disjointness, the two parties must exchange $\Omega\left(\frac{n}{k^2}\right)$ qubits.

Q. What is the right bound? Can we push the lower bound closer to the upper bound $O\left(\frac{n}{k} \log \frac{n}{k^2}\right)$?

Q. If A sends only r qubits, then how many qubits must B send? Is the answer $\Omega(n - r^2)$ for small r?